Some Remarks on Security of Receipt-Free E-auction

Her, Yong-Sork
Graduate School of Information Science and Electrical Engineering, Kyushu University

Imamoto, Kenji
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu University

出版情報：Proc. of International Conference on Information Technology and Applications 2005. Ⅱ, pp.500-563, 2005-07. IEEE Computer Sydney
バージョン：
権利関係：

Some Remarks on Security of Receipt-free E-auction

Yong-Sork Her*, Kenji Imamoto*, Kouichi Sakurai**
** Graduate School of Information Science and Electrical Engineering, Kyushu University*
*** Faculty of Information Science and Electrical Engineering, Kyushu University*
6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan
**{ysher, imamoto}@itslab.csce.kyushu-u.ac.jp, ** sakurai@csce.kyushu-u.ac.jp*
Tel: +81-92-642-3867, Fax: +81-92-632-5204
<Topic: Security>

Abstract

Recently, a receipt-free scheme is rising for a secure e-auction. The goal of a receipt-free scheme in an e-auction is to prevent a bid-rigging. If the bid-rigging happens in the e-auction, the winner can get the bidding item with an unreasonably low price. The first receipt-free scheme for the e-auction was proposed by Abe and Suzuki. Chen, Lee and Kim also proposed the extended receipt-free scheme. In this paper, we point out that the proposed receipt-free schemes do not prevent perfectly the bid-rigging attack. Moreover, we indicate that a bid-collision is a possible cause of an e-auction. In the strict sense, the bid-collusion is different from the bid-rigging. In this paper, we do not present the scheme which can prevent the bid-collision attack. We compare the bid-rigging attack with the bid-collusion attack, and analyze the security of the existed receipt-free schemes in a viewpoint of the bid-rigging attack and the bid-collusion attack.

Keyword: E-auction, Security, Receipt-freeness, Bid-rigging, Bid-collusion, Cryptography,

1. Introduction

1.1. Background

Recently, a receipt-free scheme is rising in field of e-voting [BT94,SK95,HS00] and e-auction [AS02, CLK03]. The receipt-free scheme of e-voting means that a voter should not prove other parties or people how he voted. It is known that the receipt-free scheme of e-auction is to prevent bid-rigging. Abe and Suzuki [AS02] proposed firstly the receipt-free scheme for an e-auction. They introduced the reason why the receipt-free scheme is required in an e-auction as follows.

The coercer orders other bidders to bid very low price, he then can win the auction at an unreasonably low price. To make other bidders obey his order, the coercer punishes bidders who do not cast the ordered bidding price, and the buyer rewards for bidders who cast the ordered bidding price.

The goals of the coercer are that he becomes the winner and wants to buy the auction item with an unreasonably low price. Chen, Lee and Kim [CLK03] pointed out that the receipt-free scheme of Abe and Suzuki does not provide a receipt-free for a winner. Also, they proposed a new receipt-free scheme. Table 1 shows the security of proposed receipt-free schemes.

1.2. Our contribution

In this paper, we analyze the security on the existed receipt-free e-auction. Although the coercer is the winner, the bid-rigging can succeed under the existed receipt-free scheme. Then, the receipt-free scheme is meaningless. That is, the known receipt-free schemes do not prevent the bid-rigging perfectly.

Moreover, we present a bid-collusion attack in e-auction. The bid-collusion means that all the bidders have a prior consultation on a winner and a winning price with an unreasonably low price. Therefore, all the bidders know the estimated winner and winning price. They can check whether their promise is kept or not. If their promise is kept, the winner rewards for other bidders. Otherwise, the winner is punished by other bidders. To prevent the bid-collusion attack is the bidder should not prove whether he cast a bid or not. We call *bidding-freeness*. Table 2 shows that although the existed receipt-free scheme can prevent partly the bid-rigging attack, but does not prevent the bid-collusion attack at all.

Table 1. Receipt-freeness of the existed receipt-free e-auctions

Scheme	Receipt-freeness	
	Winner	Losing Bidders
[AS02]	No	Yes
[CLK03]	Yes	Yes

Table 2. Security analysis in a viewpoint of bid-rigging and bid-collusion

	Receipt-freeness		Bidding-freeness	
[AS02]	$W = C$	No	$W = SB$	No
	$W \neq C$	No	$W \neq SB$	No
[CLK03]	$W = C$	Yes	$W = SB$	No
	$W \neq C$	Yes	$W \neq SB$	No

(*W* means Winner, and *C* means Coercer. *SB* is the Special Bidder)

2. Bid-rigging vs. Bid-collusion

In this section, we introduce the difference between the bid-rigging and the bid-collusion.

2.1 Bid-rigging

Winner = Coercer

If other bidders cast the ordered bidding price and the coercer becomes the winner, then the coercer rewards for other bidders. Although some bidders did not obey the order of the coercer, they can require a reward to the coercer, because the coercer is the winner with an unreasonably low price. Then, other bidders do not need to prove his bidding price. That is, it does not need the receipt-free scheme.

Winner ≠ Coercer

If the coercer is not the winner, he looks for the winner. Then, it needs the receipt-free scheme. And, it can be happen the dispute that the bidders who cast the ordered bidding prices can require a reward to the coercer. To success the bid-rigging, it needs two conditions as follows:

- The coercer should control all the bidders in e-auction.
- The coercer should not perform non-reputation.

2.2 Bid-collusion

The bid-collusion means that all the bidders have a prior consultation on the winner and the winning price. Therefore, all the bidders know the estimated winner (special bidder) and winning price.

Winner = Special Bidder

If the special bidder is the winner, he should reward the other bidders. Then, the other bidders do not need to prove their bidding prices. This case is same with 'winner = coercer' of bid-rigging.

Winner ≠ Special Bidder

All the bidders know the estimated winner and winning price, and know whether it keeps their promise or not. If the special bidder is not the winner, the other bidders punish the winner who broke their promise. To prevent the bid-collusion attack, it is required that a bidder should not prove he cast a bid. We call this method *bidding-freeness*. In table 3, we compare the bid-rigging attack with the bid-collusion attack.

Table 3. Comparison of Bid-rigging and Bid-collusion

Attack	**Bid-rigging**	**Bid-collusion**
Control	Coercion-control	Self-control
Control contents	Bidding price	Winner and Winning price
Corresponding method	Receipt-freeness	Bidding-freeness

3. Review of Abe-Suzuki model and Chen-Lee-Kim Model

In figure 1,2 and 3, we compare Abe-Suzuki model with Chen-Lee-Kim model by each phase.

4. Security Analysis in a viewpoint of Bid-rigging

4.1. Winner = Coercer

In case of Abe-Suzuki model, the winner and the winning price are published by auctioneers. If the coercer becomes the winner, he rewards for other bidders who obey his order without proving other bidders' bidding price. Moreover, the coercer can not perform non-repudiation. That is, the receipt-freeness is meaningless in this case. In case of Chen-Lee-Kim model, only the winning price is published. A bidder does not know who the winner is. Therefore, the receipt-freeness is protected unless the seller publishes the winner. Moreover, the coercer which is the winner can perform non-repudiation. It can be happened the argument on the winner.

4.2. Winner ≠ Coercer

All the bidders know the winner in Abe-Suzuki model. If the coercer is not the winner, the coercer inflicts punishment upon the winner. Also, some bidders who cast the ordered bidding price cry for a reward to the coercer. But, they can not prove his

Abe-Suzuki Model	Chen-Lee-Kim Model
- ***a*** auctioneers : $\{A_i \mid i = 0,\cdots,a\}$ - ***b*** bidders : $\{B_j \mid j = 0,\cdots,b\}$ - Price list : $P = \{l \mid l = 0,\cdots,m\}$ - Large primes : $p(=2q+1)$, q - A generator g of order q subgroup of Z^*_q - Messages $M_0, M_1 \in Z_q$, that mean "I do not bid", "I bid" respectively.	- ***m*** bidders : $\{B_i \mid i = 1,2,\cdots,m\}$ - Seller *S*, Auctioneer *A*, Auction Issuer *AI* - Large primes : p, $q \mid p-1$ - A subgroup G_q of order q subgroup of Z^*_q - g is a generator of G_q - Messages $G_1, G_2 \in G_q$, which mean "I bid", "I do not bid" respectively.

Fig. 1 Preparation step of the proposed receipt-free models

Abe-Suzuki Model	Chen-Lee-Kim Model
- A Bidder chooses his secret key $x_j \in Z_q$, public key $h_j = g^{x_j}$, bidding price $p_j \in P$, and secret seeds $r_{l,j} \in Z_q$ $(l = 1,2,\cdots m)$ randomly. - The bidder computes a sequence of chameleon bit-commitments $C_{l,j} \begin{cases} g^{M_1} h^{r_{l,j}} & (l = p_j) \\ g^{M_0} h^{r_{l,j}} & (l \neq p_j) \end{cases}$ For $l = 1,\cdots,m$. - The bidder proves to each auctioneer that bidder knows the secret key $\log_g h_j = x_j$ and the discrete logs $\log_g C_{i,j}$ by the interactive zero-knowledge proof. - The Bidder makes *t*-out-of-*a* secret shares $r^i_{i,j}$ for secret seeds $r_{i,j}$, and sends *i*-th shares $r^i_{i,j}$ $(i = 1,2,\cdots,m)$ of secret seeds $r^i_{i,j}$ $(i = 1,2,\cdots,m)$ with his signature to *i*-th auctioneer through the one-way untappable channel	- A bidder chooses his secret key x_{B_i}, public key $h_{B_i} = g^{x_{B_i}}$, bidding price $p_i \in P$. - The bidder computes the encrypted bidding vector $C_{l,j} = (x_{i,j}, y_{i,j})$ $= \begin{cases} (g^{a_{i,j1}}, (h_1 h_2)^{a_{i,j}} G_1), & if \quad j = p_i \\ (g^{a_{i,j1}}, (h_1 h_2)^{a_{i,j}} G_2), & if \quad j \neq p_i \end{cases}$ - The seller generates the receipt-free bidding vector $C^*_{i,j} = (x^*_{i,j}, y^*_{i,j}) = (x_{i,j} u_j, y_{i,j} v_j)$, where $u_j = g^{\beta_j}$ and $v_j = (h_1 h_2)^{\beta_j}$. - They jointly generate the proof of the validity of the bidding vector. - The bidder B_i sends $C^*_{i,j}$, P_1 and P_2 to the corresponding fields of the bulletin board. - P_1 and P_2 are a kind of proof value. For detail, see [CLK03]

Fig. 2 Bidding step of the proposed receipt-free models

bidding price. It can be happened by the argument on the winner. In case of Chen-Lee-Kim model, the receipt-free is protected unless the seller publishes the winner.

5. Security Analysis in a viewpoint of Bid-collusion

We assume that the special bidder is in collusion with other bidders. All the bidders know the estimated winner and winning price. The special bidder can be rotated by an auction item.

5.1. Winner = Special Bidder

We assume that the special bidder is the winner. The special bidder rewards for other bidders who cast a bid. Then, other bidders do not need to prove their bidding prices. Only, he should prove the fact that he made a bid to a special bidder. In case of Abe-Suzuki model, a bidder knows his secret key $x_j \in Z_q$, public key $h_j = g^{x_j}$, bidding price $p_j \in P$, and secret seeds $r_{l,j} \in Z_q$ $(l = 1,2,\cdots m)$ randomly. Therefore, he can prove his chameleon bit-commitments $C_{l,j}$ to the special bidder.

In case of Chen-Lee-Kim model, a bidder B_i sends $C^*_{i,j}$, P_1 and P_2 to the corresponding fields of the bulletin board. After the e-auction system is over, the bidder can prove $C^*_{i,j}$ to the special bidder because he knows used x_{B_i}, public key $h_{B_i} = g^{x_{B_i}}$, bidding price $p_i \in P$ and the encrypted bidding vector $C_{i,j}$.

Abe-Suzuki Model	Chen-Lee-Kim Model
- All auctioneers iterate the following steps for each price $l = m, m-1, \cdots, 1$ to determine winning (maximum) bidding price $P_{\min} = \max_j \{p_j\}$ and winning bidders. - Each auctioneer publishes shares $r^i_{i,j}$ $(j = 1,2,\cdots,b)$ of l-th secret seeds $r_{i,j}$ and check the following equalities $C_{i,j} = g^{M_1} h^{r_{i,j}}$, $(j = 1,2,\cdots,b)$ for all bidders B_j. - If there exist j's for which the above equality holds, auctioneers publish that the winning bidders are these B_j's and their winning price p_{win} is l, and stop opening.	- *AI* and *A* compute the auction result. - Let $j = n$. *AI* and *A* compute separately the final price vector $(X_i, Y_i) = (\sum_{i=1}^{m} x^*_{i,j}, \sum_{i=1}^{m} y^*_{i,j})$ - They then separately publish $X^{x_1}{}_j, X^{x_2}{}_j$ and provide a non-interactive zero-knowledge proof of common exponent with their public key h_1, h_2. Let $R_j = Y_i / X^{x_1+x_2} = G_1^{l_j} G_2^{m-l_j}$ where $0 \le l_j \le m$. - If $l_j = 0$, $j = j - 1$; else terminated. - *AI* and *A* determine the first j which satisfies $j \neq 0$, and winning price is the certain j, denote P_w. - *AI* and *A* publish the winning price P_w.

Fig. 3 Opening step of the proposed receipt-free models

5.2. Winner ≠ Special Bidder

We assume that the special bidder does not the winner. This means that the promise of all the bidders is broken. In case of Abe-Suzuki model, the winning price is published and all auctioneers know the estimated winning price. All the bidders can compare the published winning price with the estimated winning price. Other bidders inflict punishment upon the winner who broke their promise. In case of Chen-Lee-Kim model, only the winning price is published at bulletin board. Therefore, Chen-Lee-Kim model does not prevent the bid-collusion attack as that of Abe-Suzuki model.

6. Conclusions

In order to prevent the bid-rigging attack, the receipt-free schemes have been proposed. The first receipt-free e-auction was proposed by Abe and Suzuki. Also, Chen-Lee-Kim proposed the extended receipt-free scheme. In this paper, we point out that the existed receipt-free schemes do not prevent the bid-rigging attack perfectly. Moreover, we indicate that the bid-collusion is a possible cause of an e-auction. In this paper, we introduce the difference between the bid-rigging and the bid-collusion. To prevent the bid-collusion, a bidder should not prove he cast a bid. We call this method bidding-freeness. We analyze the security of the existed receipt-free schemes in a viewpoint of the receipt-freeness and the bidding-freeness. However, we do not give the bidding-free scheme in this paper.

Acknowledgement

The research was partly supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Research on System LSI Design Methodology for Social Infrastructure) of the Ministry of Education, Science and Culture (MEXT), and by the 21st Century COE Program 'Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering'.

References

[BT94] J. Benaloh and D.Tuinstra, " Receipt-Free Secret-Ballot Elections", Proc. of STOC'94, 1994.

[SK95] K.Sako and J. Kilian, "Receipt-Free Mix-type Voting Scheme", Proc, of Eurocrytpt'95, LNCS 921, Springer-Verlag, pp393-403, 1995.

[HS00] M.Hirt and K.Sako, "Efficient receipt-free voting based on homomorphic encryption", Eurocrypt 2000, LNCS 1807, pp539-556, 2000.

[AS02] M.Abe and K.Suzuki.: Receipt-Free Sealed-Bid Homomorphic Encryption, Proc. Of Public Key Cryptography2002, LNCS 2274, 191–199

[CLK03] A.Chen, B.C.Lee and K.J.Kim.: Receipt-Free E-auction Scheme Using Homomorphic Encryption. Proc. of ICISC2003, 275–290